REMARKS

In the Office Action mailed April 4, 2005, the Examiner withdrew the previous rejection of claims 1-22 and 52-58. Applicants wish to thank the Examiner for reconsideration and withdrawal of these rejections. In the Examiner's new search, a new ground of rejection along with newly cited art was provided for the Applicants to consider. Applicants have carefully considered the cited art and believe the claims remain allowable for at least the reasons mentioned below. For example, the cited art alone or in combination does not teach or suggest the aforementioned claims and has an effective date subsequent to the date of conception of the instant invention.

The Examiner cited Win (U.S. Patent 6,161,139) as a basis for rejecting claims 1, 15, 16, 18-22, 52, and 54-57 under 35 U.S.C.102(e). Win concerns a system for authenticating a user with a pair of "cookies" (Col. 8, lines 9-16) and subsequently providing the user access to various applications or resources (Col. 11, lines 28-50) as long as the "cookies" have not expired or timed-out (Col. 10, lines 50-60). Initially, the user provides a login and password to a central "access server" (Col. 9, lines 36-38) via a web browser for an initial authentication that occurs on a "registry server" (Col. 9, lines 36-41). The registry server simply compares the login and

password with a predetermined registered login and password already on the registry server database. (Col. 9, lines 39-40).

If the initial authentication with the conventional login and password succeeds, Win has the "authorization server" obtain profile information for the user including the user's name, locale information, IP address and roles (Col. 10, lines 34-38). This profile information is combined together by the authorization server to then create (1) a user cookie – containing the user's IP address (Col. 8, lines 10-13) and (2) a roles cookie – containing a list of the user's roles in the system (Col. 10, lines 40-41). Collectively, the cookies in Win are used as "day passes" for rapid authentication of the user and permission determination when requesting access to various systems and application and the avoiding repeated authentication during a time period. Indeed, cookies may be encrypted and/or digitally signed and then returned to the browser making the initial request in Win but this is not for encrypting the data (Col. 10, lines 42-45). Instead, cookies are encrypted for information integrity or tamper-evident purposes and not privacy. Win admits that encryption of the cookies is used because it is faster but signing could also be used for authentication if the added delay were tolerable.

Win uses encryption but is not concerned with keeping the content of the cookies secret. Encryption is used in Win to help ensure that the cookies are authentic and have not been tampered with by the user (Col. 8, lines 30-36). For example, Win suggests testing if a user has been authenticated by testing to see if the "user cookie" can be decrypted and then whether an IP address found inside the decrypted cookie matches the IP address expected for the user (Col. 8, lines 10-13; Col. 21, lines 65-67; Col. 22, 1-3). Likewise, the authentication is determined by testing if the "roles cookie" can be decrypted (Col. 8, lines 28-34) and then whether the combination of roles associated with the user matches an "Access Rule" Boolean expression (Col. 8, lines 34-36). If signatures were used instead of encryption, the servers would have to verify the signatures instead of just decrypting the cookies. Win points out, and it is generally accepted, that verifying digital signatures is much slower than decrypting, and thus would place an undue computational burden on the servers. If either the decryption or signature verification tests is not passed, the user is denied access to resources and information and no data passes+ (Col. 8, lines 28-36).

Once a user is authenticated and authorized to access certain resources with the cookies, a "personalized menu server" in Win creates a customized menu (or list) *showing* only those resources that the user is authorized to access (Col. 11, lines 39-45). Win uses a customized

menu to limit access to certain predetermined resources but makes no mention of selectively or individually encrypting the resources to maintain confidentiality. The cookies in Win do not contain cryptographic key material for use in a system for selectively encrypting any information.

Win mentions using SSL (Secure Socket Layer) encryption to keep the stream of information passing between web browsers and servers confidential at the "session layer". Unfortunately, the SSL-based encryption of session data has nothing to do with **selectively** encrypting delivery of the individual files or parts of files or other information transmitted to or from the user and the system (Col. 27, lines 56-61). On the contrary, **all** transactional information transmitted between a browser and HTTP server including "cookies", passwords, logins and any other data in the session is encrypted (Col. 22, lines 15-30). This rather conventional use of SSL is not new or unusual to Win.

Encrypting entire information streams of data via SSL or even a VPN (Virtual Private Network) is commonplace but is of limited usefulness because all information ends up in the clear (not encrypted) on the user's system. Win simply does not provide for selectively encrypting or decrypting individual files or parts of files but the entire session layer using SSL.

Moreover, Win does not provide for selectively encrypting or decrypting individual data objects at the "application" layer or highest layer of the protocol stacks.

Nonetheless, the Examiner rejected Claim 1 under 35 USC 102(e) as anticipated by Win. Unfortunately, the rejection of Claim 1 failed to establish the prima facie case of anticipation as each and every element of claims 1, 15, 16, 18-22, 52, and 54-57 are not taught or suggested by Win. See Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 U.S.P.Q.2D (BNA) 1913, 1920 (Fed. Cir.), cert. denied, 493 U.S. 853, 107 L. Ed. 2d 112, 110 S. Ct. 154 (1989) (explaining that an invention is anticipated if every element of the claimed invention, including all claim limitations, is shown in a single prior art reference). See Jamesbury Corp. v. Litton Industrial Products, Inc., 756 F.2d 1556, 1560, 225 USPQ 253, 256 (Fed. Cir. 1985) (explaining that the identical invention must be shown in as complete detail as is contained in the patent claim). See Verdegaal Bros., Inc. v. Union Oil Co., 814 F.2d 628, 631, 2 U.S.P.Q.2D (BNA) 1051, 1053 (Fed. Cir. 1987) (explaining that a prior art reference anticipates a claim only if the reference discloses, either expressly or inherently, every limitation of the claim). See Kloster Speedsteel AB v. Crucible, Inc., 793 F.2d 1565, 1571, 230 U.S.P.Q. (BNA) 81, 84 (Fed. Cir. 1986) ("Absence from the reference of any claimed element negates anticipation.")

By way of this rejection, the Examiner implies that Win receives a request for an access permission security profile or "cookie" on behalf of a user (Col. 9, lines 25-45) and then authenticates the request (Col. 9, lines 36-45; and Column 10, lines 26-40). Indeed, it may be true that Win indirectly receives a request for the cookie and then authenticates the request from a user. However, the "cookie" in Win is not created "to be used in forming a cryptographic key for enabling the network user to decrypt **select** portions of an encrypted object and to encrypt **selected** portions of a plaintext object" as recited in Claim 1.

It is neither taught or suggested in Win that the cookies should be used for encryption, decryption or "forming a cryptographic key" for either of these functions; instead the cookies (encrypted or digitally signed) are expressly for authentication and authorization and are only encrypted to prevent counterfeit cookie's from being created. (Col. 8, lines 10-13; Col. 10, lines 40-41). This is a subtle but important distinction. As previously described, Win authenticates a user with a "user cookie" and then determines authorization for accessing certain resources or applications with a "roles cookie". In practice, the cookies in Win are used to facilitate the building of customized menus transmitted through SSL but arriving in plaintext to any and all users of a computer; the data making up the customized menus is not selectively encrypted for certain users depending on their roles.

Further, the roles cookie helps create menus or lists displaying only those resources users have access to according to their role (Col. 11, lines 29-50). The customized menu provides a degree of security for information not through encryption but through obfuscation. That is, the Win patent attempts to keep information secure by "hiding" information behind a web server and then restricting access to the information through the presentation of a customized menu or list.

Even if Win or another reference hypothetically did use cookies for encryption or decryption of data objects, there is nothing in Win or other references cited that teaches or suggests "to decrypt selected portions of an encrypted object and to encrypt selected portions of a plaintext object" as recited in Claim 1. In fact, Win teaches away from selectively encrypting or decrypting individual objects or parts of objects as recited in Claim 1. Rather, Win only mentions using conventional and well-known session-level encryption with SSL to encrypt everything in the session exactly the same way. Win describes using SSL for *all* transactional information transmitted between a browser and HTTP server including "cookies", passwords, logins and any other data (Col. 22, lines 15-30).

With regards to Claim 15, this dependent claim is not only patentable on its own but by virtue of its dependence on allowable Claim 1.

Claim 16 is also allowable by virtue of its dependence of allowable Claim 1. For example, the token in Claim 16 is used in forming a cryptographic key used for encryptiong an decryption while the "cookies" in Win are for authentication types of operations.

Likewise, Claim 18, 19, 20, 21 and 22 are independently allowable as well as allowable by virtue of their dependence on allowable Claim 1.

With regards to independent claim 52, Win also does not teach or suggest "means for utilizing the cryptographic capabilities provided by said member token for selective encryption and decryption" as recited in amended claim 52. As previously described, the "cookies" in Win are only *used to authenticate* the user for various system resources and not to provide encryption and decryption capabilities.

Applicant respectfully submits that authentication is separate and apart from encryption and decryption capabilities. Authentication is a process of verifying the identity of a person or business, while encryption operates to convert data or information into a private form. The encrypted data once converted cannot be read or used as originally intended unless the reverse operation of decryption is applied first. In this case, Win uses "cookies" for authentication and encrypts and decrypts cookies for enhanced authentication purposes. Cookies alone are not used for cryptographic key formation and selective encryption and decryption of data.

Dependent claims 54-57 are also patentably distinct and in condition for allowance independently as well as by virtue of their dependence on allowable Claim 52.

For at least these reasons above, the Applicants would respectfully request the Examiner to withdraw the rejection of Claims 1, 15, 16, 18-22, 52, and 54-57 under 35 U.S.C.102(e) in view of Win.

In addition, the Examiner rejected claims 2-16, 18-22, 57 and 58 under 35 USC 103(a) over Win in view of Berson (U.S. Patent 6,754,821). First, these claims remain patentably distinct over Win by virtue of their dependence on allowable independent claims 1 and 52 for at least the reasons described previously. For at least this reason, the Examiner has failed to establish a prima facie case for rejecting claims 2-16, 18-22, 57 and 58 under 35 USC 103(a) which specifies:

"To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. In re Vaeck , 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)"

Accordingly, the Applicants respectfully requests that the Examiner withdraw the rejection of claims 2-16, 18-22, 57 and 58 under 35 USC 103(a) over Win in view of Berson for failing to teach or suggest each and every claim limitation.

Second, the Applicants note upon careful inspection of Berson that their conception date precedes the critical filing date of June 19, 2000. This eliminates Berson as a reference. According to Rule 37 CFR 1.131, the Applicants can eliminate the Berson reference as a basis of a rejection by providing satisfactory evidence of facts that they have a conception date prior to the effective filing date of June 19, 2000. Moreover, by the Examiner's own statements, Win taken without Berson does not teach or suggest each and every element of claims 2-16, 18-22, 57 and 58. Together, this necessarily means that at the time the invention was made the subject matter as a whole would not have been obvious. (In re Eickmeyer ,602 F.2d 974, 202 USPQ 655, 660 n.9 (C.C.P.A. 1979) (quoting In re Tanczyn, 347 F.2d 830, 146 USPQ 298, 300 (C.C.P.A. 1965)). Applicants respectfully submit the attached affidavit under Rule 37 CFR 1.131 to establish this earlier conception date and therefore request withdrawal of any and all rejections under 35 U.S.C § 103(a) made in view of Berson.

To meet the signatory requirements for 37 CFR 1.131, MPEP 409.03 Unavailability of Inventor 37 CFR 1.47 indicates that a co-inventor may sign for a non-signing inventor if a joint

inventor cannot be reached after diligent effort. In this case, we have tried diligently to locate Mr. Yu but it appears that he may have moved to China in 2005. Furthermore, none of his colleagues at SiVault (the assignee of the instant case) or Viaquo have either an address or an email address or a phone number to contact him, and therefore we are submitting this declaration without his signature. In the event the Examiner requires Mr. Yu's signature, we would be able and amenable to providing as soon as Mr. Yu moves back to the United States and/or we can discover how to get in contact with him.

Additionally, the Examiner rejected Claim 17 under 35 U.S.C. 103(a) as obvious over Win in view of Woodward (Woodward, John, "Comments on Private Sector Use of Biometrics and the Need for Limited Government Action", 7/17/1998, pp. 1-12). Applicants respectfully disagree that any motivation to combine Woodward with Win exists and therefore the prima facie case of obviousness has not been established. Moreover, Claim 17 is not only independently patentable but remains patentable by virtue of its dependence on allowable Claim 1 as described previously. ("If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious." *In re Fine*, 837 F.2d 1071, ___, 5 USPQ2d 1596 (Fed. Cir. 1988)).

The Examiner also rejected Claim 17 under 35 U.S.C. 103(a) as obvious over Win in view of Berson and further in view of Woodward. Once again, Applicants disagree that any motivation has been established to combine Win and Woodward let alone Win, Woodward and Berson together. Nonetheless, the Applicants have effectively eliminated Berson and respectfully request withdrawal of this rejection even if this combination of three disparate references were possible.

Further, the Examiner rejected Claim 53 as obvious over Win in view of Shintani (U.S. Patent 6,137,480). Applicants respectfully submit that the Examiner has failed to establish a motivation to combine Win with Shintani and the corresponding prima facie case of obviousness. Even if there were a motivation to combine these two references, dependant Claim 53 remains non-obvious and allowable as it depends from allowable Claim 52 for reasons previously described. Combining Win in view of Berson and further in view of Shintani also fails to render Claim 53 obvious not only for a lack of motivation to combine but also because Berson has an effective filing date subsequent to the invention hereof.

In summary, Applicants respectfully request reconsideration and withdrawal of the rejections for claims 1-22 and 52-58 for at least the following reasons. The Win reference alone does not anticipate claims 1, 15, 16, 18-22, 52, and 54-57 under 35 U.S.C.102(e). In addition,

Claims 2-16, 18-22, 57 and 58 under 35 USC 103(a) remain patentably distinct over Win in view of Berson as the effective filing date of Berson is subsequent to the conception of the present invention thereof. Finally, dependent Claims 17 and 53 remain independently patentable as well as patentable by way of their dependence on allowable independent Claims 1 and 52 respectively.

///

///

///

///

///

///

///

///

///

///

///

///

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 24 of 24

///

///

///

The Applicant has made a diligent effort to place the claims in condition for allowance, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Leland Wiesner, Applicants' Attorney at (650) 853-1113 so that such issues may be resolved as expeditiously as possible.

For these reasons provided above, this application is now considered to be in condition for allowance and such action is earnestly solicited.

Respectfully Submitted,

Leland Wiesner

June 8, 2006
Date

Leland Wiesner
Attorney/Agent for Applicant(s)
Reg. No. 39424

Wiesner and Associates
366 Cambridge Ave.
Palo Alto, California 94306
Tel. (650) 853-1113

Attached: 37 CFR 1.131 Affadavit by Sweet et al (115 pages).